**Statement for the Record**

**David E. Jarrell**
**Manager, Critical Infrastructure Protection Program**
**Office of the Chief Information Officer**
**U.S. Department of Commerce**

**Before the**

**United States House of Representatives**
**Committee on Homeland Security**
**Subcommittee on**
**Emerging Threats, Cybersecurity and Science and Technology**

**April 19, 2007**

## DAVID E. JARRELL, MANAGER, CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Chairman Langevin**,** Ranking Member McCaul, Chairman Thompson, Ranking Member King, and distinguished members of the Subcommittee, I appreciate the opportunity to address you on the state of cyber security protecting the Department of Commerce (Commerce).

The Commerce Information Technology (IT) security program ensures that adequate controls are in place to protect the confidentiality, integrity, and availability of non-national security and national security IT systems and the data they process, transmit, and store. To fulfill the Departments requirements under the Federal Information Security Management Act (FISMA) of 2002, the IT Security Program establishes a framework of policies and procedures consistent with government-wide laws and regulations, ensures systems are categorized and assessed for risk of harm, conducts periodic monitoring of control effectiveness, monitors tracking and completion of corrective actions, and trains personnel with IT security responsibilities.

Commerce consists of 13 bureaus that support its mission goals and objectives. This written testimony and my oral testimony will focus on the cyber intrusion affecting the Department's Bureau of Industry and Security (BIS), Commerce coordination with the Department of Homeland Security (DHS), United States – Computer Emergency Readiness Team (US-CERT), and the Department of State (State), and will offer a broad perspective of the Commerce IT security program.

## PREVENTIVE MEASURES & SECURITY POSTURING

Commerce and its bureaus work diligently to ensure a sound and comprehensive IT security program. To that end, Commerce IT personnel ensure compliance with Federal requirements such as the FISMA, Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources, Government Accountability Office (GAO) guidance, as well as guidance issued for use within Federal civilian government Departments and Agencies and throughout the IT system development life cycle. That guidance comes in the form of National Institute of Standards and Technology (NIST) Special Publications. Other guidance considered when designing and deploying operational IT systems is derived from industry services, capabilities, and best practices.

IT systems designed to support the business needs of the Department are typically managed within the program for which they will be utilized. The systems are also reviewed by the Department's Chief Information Officer (CIO) Council and/or Commerce IT Review Board (CITRB) before funding and other resources are allocated to support the system's development and integration into the Commerce infrastructure. It is this scrutiny that senior IT staff use to determine if adequate security planning and controls are integrated into the system development life cycle (SDLC) and enterprise architecture. In addition, other security measures are integrated into the design, implementation, and operation of all IT systems within Commerce.

Commerce's enterprise architecture and IT Security Program Policy and Minimum Implementation Standards require the integration of security infrastructure for in-depth control, both at the perimeter and within the program's infrastructure. Examples of the infrastructure include the use of robust router and firewall technology, vulnerability scans and penetration testing of IT systems, monitoring of firewall and Intrusion Detection and Prevention System logs, email filtering, spam filters, anti-virus software, and intrusion detection and prevention systems.

A management control implemented throughout Commerce includes user awareness training programs, an important aspect of the Department's first line of defense. IT security awareness consists of reminders that focus the user's attention on the concept of IT security in the user's daily routine. Awareness provides a general cognizance or mindfulness of one's actions, and the consequences of those actions. Awareness activities provide the means to highlight when a significant change in the IT security program policy or procedures occurs, when an incident occurs, or when a weakness in a security control is found. IT security training develops skills and knowledge such that computer users can perform their jobs more securely, and develop relevant and necessary security skills and competencies in those who access or manage Commerce information and resources. Commerce system users are required to take computer security training on a annual basis, and all new employees/contractors to Commerce are provided training during in-processing prior to being issued a user login. In addition, IT administrators are required to take additional training courses each year that directly apply to their work related activities. We are currently assessing the option of using an Information System Security Line of Business Shared Service Center as a general security awareness training provider. This initiative is an E-Government Line of Business, managed by the Department of Homeland Security, intending to make the Government-wide IT security processes more efficient.

In addition to intra-departmental controls and counter measures, the Department ensures that key personnel remain fully aware of U.S. Government-wide initiatives and programs that affect the operation or security of its IT systems. Commerce supports U.S. Government security response and planning committees to include the National Cyber Response Coordination Group (NCRCG), the Critical Infrastructure Protection Policy Coordination Committee (CIP PCC), and the National Communications System (NCS) Committee of Principals and Representatives (COP/COR).

## COMMERCE FEDERATION OF COMPUTER INCIDENT RESPONSE TEAM

For each bureau operating within Commerce, there are established Computer Incident Response Teams (CIRTs) that provide incident response for their respective bureau. Of the 13 bureaus operating within Commerce, there are six bureaus that enable their own cyber incident response programs through the use of bureau resources, including technical staff and technology. The remaining Commerce bureaus receive cyber incident response support from the centrally managed Department of Commerce Computer Incident Response Team (DOC CIRT). The DOC CIRT continually strives to reduce incident response time and increase effectiveness.

To support this decentralized computer incident response capability, Commerce also manages a Federation of Computer Incident Response Teams - where all CIRTs within the Department are represented. This intra-Departmental forum allows all Commerce CIRTs to share information on a particular incident, discuss technology and security countermeasures, and leverage Department-wide resources in the event of a large-scale attack.

Incident reports are filed directly to the DHS US-CERT in all incidents involving Department IT resources, per FISMA, other OMB guidance, and DHS US-CERT Concept of Operations (CONOPS).

On a more global level, the DHS coordinates and manages the Government Forum of Incident Response and Security Teams (GFIRST). GFIRST is a group of technical and tactical practitioners of security response teams responsible for securing government IT systems, of which the Commerce Federation of Computer Incident Response Teams maintain membership and active participation. GFIRST members work together to understand and handle computer security incidents and to encourage proactive and preventative security practices. Through participation in the GFIRST, Commerce IT security professionals receive technical information, tools, methods, assistance and guidance on cyber issues, share specific technical details regarding incidents within a trusted U.S. government environment on a peer-to-peer level, and improve incident response operations.

## INITIAL BIS INCIDENT RESPONSE AND REPORTING

Following the Department's guidance on reporting cyber incidents, BIS worked with the Network Operations Center (NOC), and the DOC CIRT to investigate suspicious behavior on BIS logical segment of the Commerce network, and its workstations. After the BIS and Commerce NOC staff confirmed that three workstations exhibited suspicious behavior, and removed them from the network, and BIS formally reported to the DOC CIRT that a breach of security occurred. As a result of this notification, the DOC CIRT notified the Director, IT Security, Infrastructure and Technology, the CIO, and the Network Operations Center (NOC), which manages the infrastructure and "back bone" network on which BIS Internet traffic traverses. The DOC CIRT also notified the US-CERT and the Department's Office of the Inspector General (OIG).

The BIS cyber incident was discovered when the BIS Deputy Under Secretary discovered that he was unable to log into his computer upon arrival to his office on July 13, 2006, at 8:23 a.m. He immediately notified his CIO and security team, which determined that his network account was in lock-out status because three unsuccessful attempts were made to log into his account. This event was initially handled internally within BIS until such time that system staff determined it to be more significant and a reportable incident. Once determined to be an incident, as defined by Commerce policy, it was reported to the DOC CIRT.

A timeline of events was created in support of the BIS incident from a BIS, DOC CIRT, and NOC perspective:

- July 13, 2006
    - The user arrived at work and attempted to log into his computer, but discovered that the BIS system "auto-locked" his account, because failed login attempt thresholds of three attempts were reached. This prevented the user's ability to login at 8:23 a.m.
    - The user prompted the BIS internal Help Desk and computer security team to begin an investigation of the event.
    - The BIS technical staff discovered that the cause of the account lock-out was because a BIS computer attempted to access another BIS computer resource. The computer in question also attempted to execute automated processes to access two IP addresses after business hours when the authorized user of that machine was not in the office.
    - Examination of the installed anti-virus client logs revealed detected and deleted programs installed on the workstation. These auto-delete actions initiated by the anti-virus client occurred at approximately the same time that the BIS user's account was locked-out.
    - The BIS technical team contacted the Commerce NOC and requested analysis of firewall logs for the previous night's IP traffic. During this stage of the investigation, the NOC found two additional BIS computers attempting to contact one of the questionable IP addresses.
    - All three infected BIS computers were removed from the network, powered down, and quarantined.

  - The BIS CIO contacted the Commerce CIO to brief him of the situation and circumstances surrounding the event, and to advise that a CIRT report was being written based on the information gathered during the day and evening, and would be filed consistent with Department procedures.
- July 14, 2006
  - BIS formally filed the incident report with DOC CIRT that identified three of its machines operating on the BIS local area network at 11:51 a.m.
  - The DOC CIRT captured forensic images of the infected computers. The DOC CIRT determined the cause of the user account lock-out was likely due to the use of the "net" command, which is used in Windows networked environments to connect to other network resources.
  - The DOC CIRT reported the BIS incident to the US-CERT at 11:55 a.m.
- July 19, 2006
  - The Commerce OIG was notified of the BIS incident at 3:15 p.m. by the Commerce Critical Infrastructure Protection (CIP) Manager
- July 20, 2006
  - The DOC CIRT requested assistance from McAfee, the company that provides Commerce anti-virus software, to analyze and provide support to identify suspicious files and to create new definition files for detection.
- July 21, 2006
  - The DOC CIRT submitted follow-up reports to the US-CERT with investigation status updates, and requested on-site technical assistance from the US-CERT at 11:48 a.m.
  - The CIP Manager advised the Department's Federation of Computer Incident Response Team of the BIS incident, and provided the "block list" of IP addresses identified as malicious or suspicious, as well as a list of malicious file names to be monitored.
- July 22, 2006
  - DOC CIRT received a definition file from McAfee which included unique signatures to detect the malicious files identified by the DOC CIRT on July 20, 2006
- July 25, 2006
  - The US-CERT provided on-site support to the DOC CIRT.
  - The US-CERT provided the DOC CIRT with updates their initial findings based on forensic image analysis.
  - The DOC CIRT requested additional assistance from McAfee to analyze and provide support to identify additional suspicious files and to create new definition files for detection.
- July 25, 2006
  - The Department of Commerce IT staff, including the DOC CIRT, continued to monitor "block list" IP addresses to ensure that unwanted and unauthorized access did not occur.
- July 26, 2006
  - DOC CIRT received definition file from McAfee with unique signatures to detect the malicious files identified by the DOC CIRT on July 25, 2006.

Throughout the course of the BIS incident investigation, blocking policies of malicious and suspicious IP addresses were imposed by the DOC CIRT, BIS technical staff, and the NOC. In addition, DOC firewall administrators and BIS technical staff reviewed archive firewall logs in an attempt to identify any previous activity fitting the characteristics of the incident. All blocks remain in place today.

In summary, Commerce and BIS became aware of the break-in to BIS computers on July 13, 2006, which was determined not to be the date of the initial infection. The firewall logs were restored from the date the incident was discovered and the preceding eight months. The DOC CIRT, BIS technical staff, and the NOC reviewed and attempted to identify the initial date of the computer system compromise, to no avail. While firewall logs were reviewed for the preceding eight months prior to detecting the BIS incident, Commerce cannot clearly define the amount of time the perpetrators were inside its BIS computers before their presence was discovered. BIS has no evidence to show that data was lost as a result of this incident.

## TRACKING AND CONTAINING THE OUTBREAK

An on-going challenge faced by the Department is the ability to differentiate between real and false-positive cyber security events, given the volume of system logs and information collected that must be reviewed to determine which activities are actionable.

BIS management took immediate action from the time the cyber security "*event*" was identified. Upon the determination that it was an "*incident*," BIS followed Commerce incident protocol and alerted the DOC CIRT, the NOC, and the Commerce CIP Manager. BIS management, along with others within the Department, quickly established that their initial discovery of one user account locked-out due to existing policy settings included three infected computers that attempted to establish connections with two suspicious IP addresses.

As discussed in the INITIAL BIS INCIDENT RESPONSE AND REPORTING section of this report, the incident was escalated when it was discovered that more than one computer was involved. By July 24, 2006, it was discovered that ten computers *attempted* to establish connections to six suspicious IP addresses. By August 18, 2006, through continued and aggressive monitoring by BIS, the Department's IT staff, and support from the DHS US-CERT, it was discovered that a total of 32 BIS computers and one non-BIS computer *attempted* access to eleven suspicious IP addresses, as detected by monitoring logs from the Department's firewalls. It was later found that all computers showed signs of infection.

Several of these victim computers were detected by the custom Intrusion Detection Systems (IDS) signatures put into place as part of the Commerce initial response. Of these custom signatures, several indicators were supplied by the US-CERT to create custom IDS signatures. In one notable case, a victim computer triggered a custom signature, and was immediately isolated according to the improved incident response procedures. Upon further examination, it appeared that the victim was in the process of preparing files for exfiltration, but stopped as a result of controls put in place to isolate the incident. Hence the initial actions taken by Commerce, BIS, DHS, and the US-CERT were demonstrably effective in containing the damage from the incident. Of the 330 Commerce systems that require certification and accreditation in accordance with FISMA, only two systems were affected by this incident.

FISMA and certification and accreditation (C&A) compliance offer IT management useful tools to ensure that adequate controls are considered, implemented, and tested throughout the system's life cycle. BIS did have a FISMA C&A package for its system which was reviewed by the Commerce CIO’s office at the time of the incident - the security incident could have occurred regardless of FISMA and C&A status because the incident method of attack uses Internet access to exploit un-patched zero-day-attack vulnerabilities, irrespective of the commercial computer security and network monitoring tools and standard prescribed Security Test & Evaluation (ST&E) penetration testing. This is a key point related to the BIS response, specifically the decision to segregate Internet access. It is also important to note that BIS has no evidence to indicate that BIS data has been exfiltrated or compromised.

## EFFECTING CHANGE ON COMMERCE AND BIS SYSTEMS

BIS implemented host-based measures that revealed other victim computers. Additional victim computers were discovered using host-based measures identifying Trojans found dormant on the BIS logical segment of the Commerce network before they became active. Processes developed by BIS to discover and stop unauthorized activity on their network proved extremely successful.

BIS established controls to detect and flag any computer infected with variants of those files causing compromise to the BIS logical segment of the Commerce network. As a result, the DOC CIRT and the NOC were able to identify those computers infected by the same outbreak traits, which included 33 computers. The Department was able to identify and quarantine the infected 33 computers through effective collaboration between Commerce and BIS IT staff involved in the incident, the “block list” of prohibited IP addresses and sites, and other controls to stop unwanted system activity (e.g., systems downloading malicious files, systems access to malicious/suspicious sites outside the control of Commerce and BIS). Only one of the 33 infected computers was outside the control of BIS.

To ensure that the infection did not spread to other Commerce bureau computer systems, file names of the infected files and associated suspicious IP addresses were shared among the Department’s Federation of Computer Incident Response Teams. After review and analysis of all system logs, no other infections or infestations were evident. In addition, all infected computer drives were quarantined from use. After sample forensic images were captured for investigative purposes, all drives were boxed and have been removed, and secured under lock and key. No data was restored from backup tape as a result of the BIS incident.

As a precautionary measure, BIS executive management required the implementation of emergency change provisions to the change management process. The change involved adding supplemental rules that created additional Virtual Local Area Networks (VLANs) assigned to BIS to segregate Internet, office automation, and export control system access, and to deny all other access for BIS VLANs. When the incident occurred, a policy was invoked to impose more stringent limits on all access to or from BIS systems, (e.g., other BIS remote sites, patch management, virus definition updates).

Custom IDS signatures capable of detecting infected files causing impact on BIS computers have remained active since the discovery of the first infected computer. These IDS safeguards, coupled with augmentation of a newly implemented Intrusion Prevention System (IPS) that monitors data streams to block and/or drop traffic based on behavior for egress and ingress to the network were instrumental in containing the damage. There is a high probability that existing backdoors, if any, to the network will be detected. In addition to safeguards put in place, BIS has added supplemental assurance by segmenting use of their logical network to ensure that computers which were connected to the BIS logical segment of the Commerce network during the attack no longer have access to the Internet – effectively segmenting computers used for BIS business processes from any Internet access. Other BIS implemented other high assurance safeguards been put in place to sustain continued and reliable operation. It is impossible to say with certainty that 100% of the infestation is eradicated from the network, but with active monitoring tools in place and an attentive IT team, there is a high probability of detection.

The DOC CIRT conducts quarterly vulnerability assessments on all devices residing on the Herbert C. Hoover Building Network (HCHBNet), which includes the BIS logical segment of the DOC network. These scans involve all devices where an IP address is assigned (e.g., server class machines, desktop computers, appliances, printers, voice phones). Internet facing systems staged on the HCHBNet Demilitarized Zone (DMZ) are also part of the quarterly vulnerability assessments. In addition to quarterly vulnerability assessments, the DOC CIRT conducts vulnerability assessments for bureaus as requested to support certification and accreditation enhancements when newly approved systems and/or network devices are ready for network integration. On average, there are approximately 14,000 checks for potential vulnerabilities factored into each assessment. Results of each assessment are shared with the bureau CIO and IT Security Officer for action. The last two quarterly scans were conducted on December 18, 2006, and again on April 13, 2007.

In supporting FISMA-required certification and accreditations, the Department spends on average between $20K and $250K for Commerce IT systems depending on the size, complexity and significance. There are a total of 330 IT systems in the Department's IT inventory. Approximations are provided since legacy systems are sometimes retired from production while new systems are introduced. Results of each system certification and accreditation security testing exercise yields extremely valuable information to the authorizing official who is ultimately responsible for the security of their system(s). Used as an education and program enhancement tool, yield valuable information pertaining to the system's overall security posture. An itemized inventory of vulnerabilities is generated during security testing that allows the system owner to methodically address as either "quick fix" items that can be readily resolved, or as mid- to long range items requiring supplemental resources. Long-term action items are inventoried in the system's Plan of Action and Milestones (POA&M).

Security testing is applied to each system as part of the System Development Life Cycle, which ensures that adequate security controls, monitoring, and logging capabilities exist, and that the overall implementation of new technology does not weaken existing security. In addition, introduction of any change is tested in a lab setting prior to being brought before the Change Control Board (CCB) for consideration, and before final integration into the production environment is allowed.

## SITUATIONAL AWARENESS BRIEFINGS

Situational awareness briefings are a tool used by the Commerce (CIO) to allow staff to receive status updates on various issues pertaining to cyber security and incident response situations occurring within Commerce. Such situational cyber security awareness briefings come in two forms: proactive and incident response briefings.

Proactive situational awareness briefings are typically scheduled for senior and technical IT professionals on a recurring basis so that they can remain apprised of cyber threats and alerts, industry recommendations, product and vendor services and capabilities, and other variables. In the realm of cyber threats and alerts, Commerce managers are informed of newly released notifications published by the DHS/US-CERT and other "watch dog" organizations that monitor and provide status on cyber-related threats and trends. As a form of proactive briefings, the CIO coordinated briefings from the DHS/US-CERT, and the Department of Defense (DoD) Joint Task Force-Global Network Operations (JTF-GNO). These briefings allowed Commerce managers to better understand the range and magnitude of cyber-related events on a global scale and the specific impacts against U.S. government managed IT systems. In all cases, Commerce IT managers have found value in the information provided by DHS/US-CERT, and DoD JTF-GNO.

Incident Response briefings are designed to inform those charged with the management and control of IT systems and resources of a particular incident and its operational impact on an affected system, its data, and the security of the system. After the BIS incident was discovered and initial response and reporting requirements were satisfied, several meetings were scheduled for the Department's senior management so that they might better understand the cyber threats faced today. To support this initiative, several briefings were scheduled that brought together Commerce senior management, the Commerce IT Security Director, the Department of Homeland Security, US-CERT management, and DoD JTF-GNO. As a supplemental effort to learn more about incidents involving U.S. Government systems, a briefing was scheduled between

Commerce and BIS IT managers, and those charged with securing the State IT systems, where a "lessons learned" discussion engaged all parties.

## INFORMATION TECHNOLOGY SECURITY ENHANCEMENTS

Monitoring and improving the state of IT security infrastructure capabilities remains a priority for the Commerce CIO. Improvements come in the form of newly released technology and upgrades to the Department's existing infrastructure. Patch management for system and appliances are updated routinely and coordinated through a formalized CCB. These changes are introduced into a test lab environment where changes and new technology can be evaluated before they are placed in a "production" environment.

To supplement the existing IPS running in IDS mode, the Department has integrated a full scale IPS to achieve active protection at the firewall. This newer technology allows the capture and analysis of both ingress and egress traffic across the network in the event of a cyber security incident. A second, more powerful log server for faster analysis and redundant storage was procured with log analysis software to speed and refine the analysis of firewall and other system logs. In addition, firewall upgrades were enabled to allow deep application inspection of traffic, and firewall log storage was increased to allow more data storage captured from the device(s).

Minimizing cyber security incident response time is a goal that the entire Federation of Computer Incident Response Team strives to improve. Changes were recently made that enable the DOC CIRT to gain direct read access to firewall logs, without intervention by the firewall administrators or other third parties, thus improving incident response time.

Commerce will play an active role in the Cyber Storm 2007. Cyber Storm is the U.S. DHS National Cyber Security Division (NCSD) national cyber exercise. The exercise is a unique government-led, full-scale, cyber security exercise supporting Homeland Security Presidential Directive 7. Commerce also participated in the first Cyber Storm 2006 exercise coordinated by DHS/NCSD.

Commerce is also working with DHS program managers to explore the integration of Project Einstein into Commerce managed systems. The US-CERT Einstein Program is an initiative that builds cyber-related situational awareness across the Federal government. The program monitors government agencies' networks to facilitate the identification and response to cyber threats and attacks, improves network security, and increases the resiliency of critical electronically delivered government services. Einstein leverages IT so that the US-CERT can automate the sharing of critical information across the entire Federal government. Enhanced data sharing between Federal government agencies and the US-CERT provides an advanced cyber view and analysis of the Federal government's critical cyber networks.

In 2008 the Department has budgeted $120 million for IT security.  This funding is estimated by the 13 bureaus operating with Commerce for a variety of IT security related tasks, including security awareness and training, system certification and accreditation, IT security operations improvements, existing security program maintenance, contingency of operations and disaster recovery planning, and other IT security related initiatives.

Thank you for the opportunity to appear before this Subcommittee today, and I would be happy to answer any questions you may have at this time.